

**Management Advisory Report: Review of
Lost or Stolen Sensitive Items of Inventory
at the Internal Revenue Service**

November 2001

Reference Number: 2002-10-030

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

INSPECTOR GENERAL
for TAX
ADMINISTRATION

November 29, 2001

MEMORANDUM FOR COMMISSIONER ROSSOTTI

A handwritten signature in cursive script, reading "Pamela J. Gardiner".

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Management Advisory Report - Review of Lost or Stolen
Sensitive Items of Inventory at the Internal Revenue Service
(Audit # 200110057)

This report presents the results of our review of the effectiveness of the Internal Revenue Service's (IRS) inventory controls over firearms, computers, and other sensitive items that, if lost or stolen, might compromise the public's safety, national security, or ongoing investigations. This review was conducted at the request of Senator Charles E. Grassley, Ranking Member of the Senate Committee on Finance.

In summary, we found that although the IRS has established procedures to control its inventory of computers, firearms, and other sensitive items, it has experienced longstanding difficulties in maintaining reliable and accurate inventory information. The IRS has reported a material weakness in inventory controls in its Annual Assurance Statement to the Department of the Treasury every year since 1983. The General Accounting Office (GAO), in its most recent audit report of the IRS' Fiscal Year 2000 financial statements, reported that serious weaknesses in the inventory system and controls continue to prevent the IRS from having equipment information available for management purposes, and from having reasonable assurance that the assets are properly safeguarded.¹ The IRS is working to acquire and implement a new inventory system to adequately account for and control its property and equipment.

For the past 3 years, the IRS reported approximately 2,300 missing computers, 5 stolen firearms and 1 lost firearm. Further, the IRS reported that, to its knowledge, no missing computers contained classified data or had an internal secure modem installed.

¹ IRS' Fiscal Year 2000 Financial Statements (GAO-01-394, dated March 2001).

Management's Response: IRS management agreed to most of the recommendations presented in the report. They plan to establish separate status codes for lost, stolen, and damaged items; generate a report and monitor the status of missing items that are coded as pending resolution; and, provide guidance on the types of lost or stolen investigative equipment that should be referred to TIGTA for investigation.

IRS management does not plan to take any further action to provide guidance on the types of lost or stolen computers that should be referred to TIGTA for investigation, believing that it already has sufficient guidance in draft procedures that were implemented in October 2001.

Management's complete response to the draft report is included as Appendix IV.

Office of Audit Comment: We encourage the IRS to update its Internal Revenue Manual (IRM) to formally incorporate these draft procedures. Also, we suggest that the IRS include these procedures in other applicable sections of the IRM and handbooks that cover property and equipment. In its response, the IRS references procedures that govern magnetic media. While we agree from a technical standpoint that hard drives on computers are magnetic media, we believe a more common interpretation of the term refers to easily removable media such as tapes and disks, and that employees would not normally look to a section on magnetic media for procedures on lost or stolen equipment.

While we still believe our recommendation is worthwhile, we do not intend to elevate our disagreement concerning it to the Department of the Treasury for resolution.

Copies of this report are also being sent to the IRS managers who are affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions or Daniel R. Devlin, Assistant Inspector General for Audit (Headquarters Operations and Exempt Organizations Programs), at (202) 622-8500.

Management Advisory Report: Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service

Table of Contents

Background	Page 1
Evaluation of the Internal Revenue Service's Inventory Regulations.....	Page 2
Identify Missing or Stolen Items of the Internal Revenue Service's Inventory.....	Page 6
Evaluation of the Internal Revenue Service's Plan to Recoup Inventory...	Page 9
Recommend Methods to Improve the Internal Revenue Service's Inventory Regulations.....	Page 10
<u>Recommendation 1:</u>	Page 10
<u>Recommendations 2 and 3:</u>	Page 11
Missing Computers Containing Classified Data.....	Page 11
Missing Computers With Access to Internal Networks.	Page 12
Appendix I – Detailed Objective, Scope, and Methodology	Page 13
Appendix II – Major Contributors to This Report.....	Page 15
Appendix III – Report Distribution List	Page 16
Appendix IV – Management's Response to the Draft Report	Page 17

Management Advisory Report: Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service

Background

This review was conducted at the request of Senator Charles E. Grassley, Ranking Member of the Senate Committee on Finance. Senator Grassley, in a letter dated September 25, 2001, voiced concerns over the controls within the Internal Revenue Service (IRS) to effectively perform its mission while protecting the integrity of its inventory of sensitive items. For purposes of his request, he defined inventory to include the IRS' stock of firearms, computers, and other items that, if lost or stolen, might compromise the public's safety, national security, or ongoing investigations.

Our review was conducted at the IRS' National Headquarters in Washington, DC during the period September through November 2001, and included the Offices of the Deputy Commissioner for Modernization and Chief Information Officer (CIO), and the Chief, Criminal Investigation (CI). The audit was conducted in accordance with the President's Council on Integrity and Efficiency's *Quality Standards for Inspections*. Detailed information on our objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

During the review, we coordinated our work with the Department of the Treasury Office of Inspector General (OIG) and the General Accounting Office (GAO), both of whom are performing similar reviews of sensitive inventory items in other Treasury bureaus and government agencies, respectively.

We also conducted a similar review within the Treasury Inspector General for Tax Administration's (TIGTA) Offices of Investigations and Information Technology. The results of that review will be reported separately.

In his request, Senator Grassley asked that TIGTA include in its assessment the following six elements:

- Evaluate whether the IRS' inventory regulations are sufficient to prevent loss or theft of its inventory.

Management Advisory Report: Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service

- Identify any missing or stolen item of IRS inventory for the past 3 years, to include that item's description and a brief explanation of the loss.
- Evaluate the IRS' plan to recoup inventory that cannot be located for the past 3 years.
- Recommend methods to improve the IRS' inventory regulations and accounting methods to prevent future loss.
- For any missing computer, state whether the computer contained classified data. In general terms, describe the nature of that data. Also, describe the IRS' plan to prevent the unauthorized dissemination of such data.
- For any missing computer, state whether the computer had internal secure modems that allowed access to internal networks. If so, state the number of missing computers that allowed for such access. Also, describe the IRS' plan to prevent unauthorized access to internal networks.

We are presenting the results of our review by separately addressing each of these six elements. The information and data we obtained are what the IRS has reported to us, and we did not independently verify the data; accordingly, we express no opinion on the accuracy or completeness of the data.

Evaluation of the Internal Revenue Service's Inventory Regulations

The IRS has established procedures to control its inventory of computers, firearms, and other sensitive items; however, the IRS has experienced longstanding difficulties in maintaining reliable and accurate inventory information, as discussed later in this report.

Computers

The CIO is responsible for maintaining an inventory of all automated data processing equipment. The inventory includes:

Management Advisory Report: Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service

- General-purpose hardware to include telecommunication equipment.
- Commercial off-the-shelf software.
- Application software.
- Communications property.

The CIO function has the responsibility for the accounting of all automated data processing equipment and is migrating to the Information Technology Asset Management System (ITAMS) to better manage the inventory. The procedures for accounting and controlling computer equipment from procurement to disposal are in the ITAMS User Guide.

In March 2001, the CIO implemented the Single Point Inventory Function (SPIF) consisting of a corporate SPIF section and local SPIF units. The corporate SPIF section has the responsibility of preparing initial information in ITAMS and the local SPIF unit has the responsibility for the equipment and the inventory database until disposal of the equipment.

During Fiscal Year (FY) 2001, the CIO function performed a physical inventory and certification to ensure that the ITAMS reflected an accurate and complete inventory of computer equipment. The inventory certification process included the preparation of a reconciliation plan for computer equipment that could not be located. The CIO function monitors the reconciliation plan until the inventory is reconciled. A *Report of Survey* (Form 1933) is used to report all lost or stolen property.

The IRS has reported a material weakness in inventory controls in its Annual Assurance Statement to the Department of the Treasury every year since 1983. The GAO, in its most recent audit report of the IRS' FY 2000 financial statements, reported that serious weaknesses in the inventory system and controls continue to prevent the IRS from having equipment information available for management purposes, and from having reasonable

Management Advisory Report: Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service

assurance that the assets are properly safeguarded.¹ In addition, TIGTA reported in November 2000 that continued involvement by senior management is necessary to sustain a reliable inventory figure and address fundamental issues that will have an impact on the long-term viability of an integrated financial management system.²

According to the IRS' September 2001 Federal Financial Management Improvement Act³ remediation plan, various actions have been completed to ensure that the IRS adequately accounts for and controls its property and equipment. Final implementation of a modernized inventory system to replace the current system is scheduled for October 2002. Further, the IRS intends to acquire a fixed asset module for its integrated financial system by March 2005.

As an additional indicator of the weaknesses in the IRS' automated data processing equipment inventory system, the IRS was unable to easily provide information concerning the number of lost or stolen computers during the course of this review. Though total counts were eventually provided, no detailed numbers of lost, stolen, or damaged items of inventory could be provided. This was due, in part, to the manner in which missing items are recorded on the inventory records. First, in general, a missing item is initially recorded as a status code "16" (Pending Resolution) while it is being preliminarily investigated. In some instances, items were left in this status without being updated for current status. Second, once an item is confirmed to be truly missing, it is recorded on the inventory as status "07" (Lost/Theft/Damaged) and forwarded for investigation. Using this all-inclusive status

¹ *IRS' Fiscal Year 2000 Financial Statements* (GAO-01-394, dated March 2001). Weaknesses in management and accounting for property and equipment are also reported in *Internal Revenue Service: Progress Made, but Further Actions Needed to Improve Financial Management* (GAO-02-35, dated October 2001).

² *The Asset Management Program Can Be Successful Through Active Executive Monitoring and Oversight* (Reference Number 2001-10-018, dated November 2000).

³ 31 U.S.C. § 3512.

Management Advisory Report: Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service

code, the IRS is unable to differentiate between items that are lost, stolen, or damaged.

Firearms and Other Sensitive Items

The Chief, CI, is responsible for maintaining an inventory of all investigative equipment. Investigative equipment includes, but is not limited to, the following:

- Firearms/Body Armor.
- Radio communication equipment.
- Electronic surveillance equipment.
- Vehicles.
- Badges/Credentials.

The CI function has the responsibility for the accounting of all investigative equipment and uses the Criminal Investigation Equipment Control System (CIECS) to manage its inventory. Procedures for accounting and controlling investigative equipment are in the CI's Property Handbook of the Internal Revenue Manual (IRM), and CIECS Operation Guidelines. Usually, items recorded on CIECS must exceed a dollar threshold, but certain items such as firearms, enforcement badges, belt badges, audio recording devices, binoculars, photo equipment, and CI commissions must be recorded on CIECS regardless of their dollar value.

The CIECS has different levels of access. Per the IRM guidelines, the CI Special Agents in Charge determine the level of access for their individual groups. The procedures for recording equipment from procurement to disposal are documented in the IRS' Property Handbook.

Property inventories are done locally on an annual basis, and the documentation from the review is maintained at the local site. Offices are divided into groups, and each group does the inventory review of another group. The Program Evaluation Office (PEO) reviews each office every 2 to 3 years. The PEO also reviews the documentation of the annual reviews and does some testing of the accuracy of the reviews.

Management Advisory Report: Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service

The CI function is required to complete an annual assurance statement, which is a self-assessment of management controls within each official's span of control and includes an evaluation of physical security in the local offices and a certification of assigned equipment. We were provided CI's last annual assurance statement dated September 5, 2001, which did not identify any significant control weaknesses. Further, our review of the documentation provided by the CI function showed that the annual inventories were being conducted in accordance with its procedures.

The CIECS cannot provide a listing differentiating between lost or stolen items of inventory. Like the IRS' computer inventory records, lost or stolen items are entered into the inventory as a status code "07." The CI function had to provide hard copy files of Forms 1933 to manually identify which items were either lost or stolen.

In addition, we were informed by CI personnel that in the future, the field offices will send in all the documentation on their inventories, including all Forms 1933, for National Headquarters review. The IRM will be updated to reflect this new requirement.

Identify Missing or Stolen Items of the Internal Revenue Service's Inventory

Our reporting of lost or stolen items involves the period October 1, 1998, through September 30, 2001, unless otherwise noted. Also, the IRS had inventory located in buildings impacted by the terrorist activities of September 11, 2001; accordingly, some numbers may not have been updated to reflect those events.

Computers

CIO personnel provided a database of 2,332 missing laptop computers, microcomputers, and micro servers for the past 3 years. This database contained the following:

- 1,236 – Status Code 07 (Lost/Theft/Damaged).
- 427 – Status Code 15 (Reserved for Facilities Management).
- 669 – Status Code 16 (Pending Resolution).

Management Advisory Report: Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service

Specific numbers differentiating between lost or stolen computers, or eliminating damaged computers, could not be provided due to the manner in which these items were recorded in the inventory, as previously discussed.

As of September 30, 2001, the IRS reported that it had approximately 163,000 laptop computers, microcomputers, and micro servers in its inventory.

Firearms and Other Sensitive Items

In consultation with CI staff, we determined that we could not rely on the CIECS to provide a reasonably accurate extract on the number of lost or stolen items due to the status code used to record these items. As an alternative, we reviewed records (Forms 1933) that the CI function provided from 32 of its 35 field offices (of the 32 offices that did provide records, 3 offices only provided records for FY 2001).

From these records, we identified 1 lost firearm, 4 stolen firearms, and 502 other investigative items that were lost or stolen. Included in the 502 other items are 50 communications devices, 40 identification badges, and 15 electronic surveillance devices that could compromise the public's safety or ongoing investigations. The remaining 397 other investigative items would not significantly compromise the public's safety, national security, or ongoing investigations. We are unable to comment on the three CI offices that did not provide records, and the fiscal years associated with the three offices that only provided records for FY 2001. Also, these numbers are exclusive of any losses pertaining to the events of September 11, 2001.

Further, we identified one additional stolen firearm during the past 3 years from investigative records maintained by TIGTA. (Three of the four stolen firearms identified through our review of CI records were also listed as investigative cases of TIGTA.) The lost firearm was not referred to TIGTA due to the circumstances surrounding the loss (see below).

Management Advisory Report: Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service

The following is a brief explanation of the one lost and five stolen firearms:

- On December 22, 1998, a Special Agent's government vehicle was broken into and his firearm and two spare ammunition magazines were stolen. The incident was reported to the local police. The incident was not reported to TIGTA.
- On March 17, 1999, a Special Agent's government vehicle was broken into and his firearm was stolen. Local police recovered the firearm on October 16, 1999. The incident was reported to TIGTA.
- On April 26, 1999, a Special Agent was involved in a boating accident and his firearm sank to the bottom of the ocean and could not be recovered. The incident was not reported to TIGTA.
- On October 21, 1999, a Special Agent's unlocked, privately-owned vehicle was entered and a pouch containing his firearm was taken. The pouch still containing the firearm was found the same day by a motorist at an intersection and turned over to the local police. We identified this stolen firearm through TIGTA's records.
- On May 3, 2000, a Special Agent's government vehicle was broken into and his firearm and other investigative articles were stolen. The firearm has yet to be recovered, and per the latest TIGTA case status, the incident is being investigated by the local police.
- On August 15, 2001, a Special Agent's government vehicle was broken into and his firearm and other investigative articles were stolen. The incident was reported to TIGTA and is being investigated by the local police.

The CI function reported no lost or stolen items of seized property for the past 3 years.

Management Advisory Report: Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service

As of September 30, 2001, the CI function reported that it had approximately 5,500 firearms in its inventory.

Evaluation of the Internal Revenue Service's Plan to Recoup Inventory

Computers

The IRS is not consistent in the way missing computers are investigated. Also, the IRS does not have written procedures requiring referrals of lost or stolen equipment to TIGTA.

CIO personnel informed us that for computers identified as missing, they record a status code of "16" into the inventory system and perform their own internal investigation. For computers they are unable to locate through their internal investigation, they record a status code of "07" into the inventory system and prepare a Form 1933, which is forwarded to TIGTA for investigation. However, based on IRS-provided data files of lost or stolen items for the past 3 years, we noticed that some items coded as "07" were not shown as being forwarded to TIGTA. Conversely, we also found items coded as "16" and "15" that were reported as being forwarded to TIGTA for investigation. Of the 2,332 missing computers, the IRS reported that 1,597 were forwarded to TIGTA for investigation.

When a missing item is reported to TIGTA, it is recorded into a database and a review is made to determine the type of action needed. The referral is either carded for a formal investigation or it is returned to the IRS for action. We were unable to confirm the accuracy of the IRS' referrals to TIGTA, since TIGTA's Office of Investigations' database of referrals does not track referrals received by specific equipment type. To fully determine the disposition of the referrals will require TIGTA's Office of Investigations to work with the IRS to review the initial referral documents in an effort to identify the course of action that was taken by TIGTA. We will continue our work in this area and respond to the Committee at a later date.

Management Advisory Report: Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service

Firearms and Other Sensitive Items

Our review of the CI function's records of lost or stolen investigative equipment, including weapons, showed that the CI function was following its policies and procedures to try to recover the equipment. For stolen property, the CI function reported the incident to the local police. For lost or stolen property, the responsible employee prepared a written description explaining the circumstances of the missing equipment, the detailed actions of what he/she did to search for the missing equipment, and the results of the search. An IRS official then determined if the employee was negligent and responsible for replacing the missing item.

Documentation of the above actions was identified in the Form 1933 file. In addition, we were told that it is the CI function's practice to report stolen equipment to TIGTA for investigative consideration.

Of the five stolen firearms, we confirmed that four were forwarded to TIGTA for investigation. A sixth firearm that was lost in the boating accident was not reported to TIGTA. The TIGTA's files showed that local police recovered two firearms and are still investigating the other two cases.

Recommend Methods to Improve the Internal Revenue Service's Inventory Regulations

Both the GAO and TIGTA have made several recommendations in prior audit reports to improve the IRS' inventory controls and systems. Based on our limited review, we further recommend that the IRS take the following actions.

Recommendations

1. Establish specific status codes to differentiate between lost, stolen, and damaged items of inventory for all IRS inventory systems.

Management's Response: The Director, Enterprise Systems Asset Management, will establish specific status codes to differentiate between lost, stolen, and damaged computers. Also, the CI function will incorporate the requirement to

Management Advisory Report: Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service

establish specific status codes to differentiate between lost, stolen, and damaged items into the new CIECS system.

2. Periodically generate from the inventory systems a report of all items of inventory that are recorded as status code "16" to ensure prompt and accurate action on these items, including a full investigation when warranted.

Management's Response: The Director, Enterprise Systems Asset Management, will generate a monthly report of all status code "16" inventory items, and will monitor to ensure prompt and accurate action on these items, including a full investigation when warranted.

3. Provide written guidance on the types of lost or stolen equipment that should be referred to TIGTA.

Management's Response: The IRS believes that it has written procedures requiring it to notify TIGTA regarding lost and stolen computers. Draft procedures were implemented in October 2001. The CI function will revise its manual to provide guidance on the types of lost or stolen equipment that management should refer to TIGTA.

Office of Audit Comment: We encourage the IRS to update its Internal Revenue Manual (IRM) to formally incorporate these draft procedures. Also, we suggest that the IRS include these procedures in other applicable sections of the IRM and handbooks that cover property and equipment. In its response, the IRS references procedures that govern magnetic media. While we agree from a technical standpoint that hard drives on computers are magnetic media, we believe a more common interpretation of the term refers to easily removable media such as tapes and disks, and that employees would not normally look to a section on magnetic media for procedures on lost or stolen equipment.

Missing Computers Containing Classified Data

The IRS reported that to its knowledge, no lost or stolen computers contained classified data.

The IRS' policy is that no classified data be maintained on employees' computers. We were advised that classified data on security vulnerabilities is maintained on two CIO,

Management Advisory Report: Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service

Office of Security laptop computers that are kept in a safe when not in use and, when in use, are only used in a secure location. We observed the safe in which the computers are maintained and the secure area in which they are used, and believe the data is adequately protected to guard against the risk of the data being stolen.

Missing Computers With Access to Internal Networks

The IRS does not use any modems that would be termed an “internal secure modem.” Therefore, access to IRS networks through any missing computers is unlikely. To gain access to IRS networks or internal database systems, one must first be able to logon to the computer itself. This entails the use of a username and password. Second, once into the IRS’ intranet, one would not only have to go through an additional logon process for a given system, but would also have to be recognized by that system as a person authorized to gain access.

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine the effectiveness of the Internal Revenue Service's (IRS) inventory controls over firearms, computers, and other sensitive items that, if lost or stolen, might compromise the public's safety, national security, or ongoing investigations. In doing so, we gathered sufficient evidence to specifically answer the questions posed in the congressional request, including the identification of any missing or stolen items for the past 3 years. To accomplish our objective, we:

- I. Developed an understanding of the IRS' policies and procedures for managing and controlling its inventory of sensitive items, including procedures to prevent the loss or theft of such items.
 - A. Obtained current inventory procedures for recording, safeguarding, and disposing of inventory items. Discussed procedures with responsible IRS officials to ensure our understanding of the procedures.
 - B. Identified controls to ensure that policies and procedures were followed.
 - C. Identified the procedures to report missing or stolen property.
 - D. Identified the procedures to recover any missing or stolen property.
- II. Determined whether the IRS' policies and procedures for managing and controlling sensitive items, including procedures to prevent the loss or theft, were effective.
 - A. Evaluated the procedures and controls with regards to providing an inventory process that is reasonable and that would provide for effective accountability to prevent the loss or theft of sensitive items such as firearms, computers, etc.
 - B. Obtained summary inventory listing of all property, and identified items that, if missing or stolen, might compromise the public's safety, national security, or ongoing investigations.
 - C. Obtained a listing of any missing or stolen items of inventory (including all seized property) for the past 3 years (October 1, 1998 to September 30, 2001), and attempted to obtain all *Report of Survey* (Forms 1933) to identify the item's description and explanation of the loss. Also, attempted to verify, with the Treasury Inspector General for Tax Administration's (TIGTA) Office of Investigations, if the items were referred to TIGTA for investigation.
 - D. Identified if any missing computers contained classified data and/or internal secure modems that would either allow for unauthorized dissemination of data or access to

Management Advisory Report: Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service

internal IRS networks. Also, identified the IRS' plans to prevent such unauthorized activity.

1. Inquired of the IRS as to whether any classified data existed within the agency, and if so, the location of such data.
 2. Documented the process to gain access to IRS automated systems through dial-in procedures.
- E. Evaluated the results of any efforts to get back missing or stolen items.
- F. Obtained physical inventory records to evaluate the extent of the inventories and to see if sensitive types of items were being identified during the physical inventory process.
- G. Obtained physical security reports to evaluate the extent to which the IRS used physical security reviews as a deterrent to theft.
- H. Identified and summarized prior TIGTA and General Accounting Office (GAO) audit findings related to IRS inventory controls, and gathered information from the Treasury's Inventory, Tracking, and Closure System and the IRS' Federal Financial Management Improvement Act¹ Remediation Plan to identify the current status of management's actions relative to the audit findings.
- I. Discussed with GAO auditors their plans for performing audit procedures during the Fiscal Year 2001 financial statement audit relative to sensitive items as described in the congressional request.

¹ 31 U.S.C. § 3512.

Major Contributors to This Report

Daniel R. Devlin, Assistant Inspector General for Audit (Headquarters Operations and Exempt Organizations Programs)
John R. Wright, Director
Thomas J. Brunetto, Audit Manager
Terrey Haley, Senior Auditor
S. Kent Johnson, Senior Auditor
Gwenevere Bryant-Hill, Auditor
Linda J. Douglas, Auditor
Bobbie M. Draudt, Auditor
Peter L. Stoughton, Auditor

Management Advisory Report: Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service

Appendix III

Report Distribution List

Deputy Commissioner N:DC
Deputy Commissioner for Modernization and Chief Information Officer M
Chief, Criminal Investigation CI
Chief Financial Officer N:CFO
Chief, Agency-Wide Shared Services A
Director, Office of Security M:S
Director, Security Evaluation and Oversight M:S:S
Director, Enterprise Systems and Asset Management M:I:E:CP:T:A
Director, Legislative Affairs CL:LA
Director, Office Program Evaluation and Risk Analysis N:ADC:R:O
Chief Counsel CC
National Taxpayer Advocate TA
Office of Management Controls N:CFO:F:M
Audit Liaisons: Deputy Commissioner for Modernization and Chief Information Officer M
 Chief, Criminal Investigation CI
 Chief Financial Officer N:CFO
 Chief, Agency-Wide Shared Services A

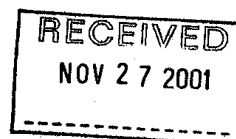
Management Advisory Report: Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service

Appendix IV

Management's Response to the Draft Report



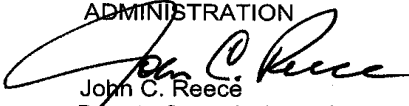
DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224



November 26, 2001

MEMORANDUM FOR TREASURY INSPECTOR GENERAL FOR TAX
ADMINISTRATION

FROM:


John C. Reece
Deputy Commissioner for Modernization &
Chief Information Officer

Subject:

Management Response to Management Advisory Draft
Report—Review of Lost or Stolen Sensitive Items of Inventory
at the Internal Revenue Service (Audit No. 200110057)

Your report evaluated the Internal Revenue Service's (IRS) Modernization and Information Technology Services (MITS) and Criminal Investigation (CI) regulations to control its inventory of computers, firearms and other sensitive items. We will use the findings and recommendations to improve our procedures and oversight of automated data processing and investigative equipment.

I would like to clarify some of the statements made in the report so the reader will have a more accurate picture of events that took place during the audit.

1. In the first paragraph of page 7, the report states that the CI function provided records from 32 of its 35 field offices; of the 32 offices that did provide records, 3 offices only provided records for FY 2001. The report should note that the additional records do exist but were not available in the short timeframe of the audit. The field office level maintains the records, but had not received all records in time for the audit.
2. On page 8, first paragraph under Computers, the report states that the "IRS does not have written procedures requiring referrals of lost or stolen equipment to TIGTA". The report should note that all computers contain magnetic media (hard drives), and in fact, it was hard drives and classified information that might be contained on those hard drives, that TIGTA reviewed. Accordingly, the loss or theft of a computer (and its media) are covered under the formally published magnetic media reporting process. See Attachment 2.

Management Advisory Report: Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service

2

3. In the last section of page 9, the report states "An IRS official then determined if the employee was negligent and responsible for replacing the missing item." The report should also note that when management found the employee negligent, management required the employee to pay for the missing item and imposed disciplinary action.

We have addressed our actions in the attached management response. If you have any questions, please contact me at (202) 622- 6800. Members of your staff can contact John Mierzeski, Acting Office Manager, Program Oversight and Coordination, at (202) 283-5987.

Attachment

cc: Associate Inspector General for Audit (Information Systems Programs)
Director, Legislative Affairs

Management Advisory Report: Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service

Attachment

Management Response to "Management Advisory Report: Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service" (Audit No. 200110057)

Recommendation #1

Establish specific status codes to differentiate between lost, stolen, and damaged items of inventory for all IRS inventory systems.

Assessment of Cause #1a

The MITS organization does not have separate status codes differentiating between lost, stolen, or damaged items (i.e., computers.)

Corrective Action #1a

The Director Enterprise Systems Asset Management will establish specific status codes to differentiate between lost, stolen, and damaged computers.

Implementation Date of Corrective Action #1a

Completed:

Proposed: January 1, 2002

Responsible Official for Corrective Action #1a

Deputy Commissioner for Modernization and Chief Information Officer M
Chief Information Technology Services M:l
Director Enterprise Systems Asset Management M:l:M

Monitoring Plan for Corrective Action #1a

Monthly, the Program Manager, Asset Management, Enterprise Systems Asset Management, will assess the implementation and effectiveness of the specific status codes that differentiate lost, stolen, and damaged computers.

Management Advisory Report: Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service

Attachment

Management Response to "Management Advisory Report: Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service" (Audit No. 200110057)

Assessment of Cause #1b

Criminal Investigation (CI) organization based Equipment Control System (CIECS) was designed using the requirements of the Property Asset Tracking system (PATS). This system required employees to combine the closing codes.

Corrective Action #1b

Criminal Investigation will incorporate the requirement, to establish specific status codes to differentiate between lost, stolen, and damaged items, into the new CIECS system.

Implementation Date of Corrective Action #1b

Completed:

Proposed: May 1, 2003

Responsible Official for Corrective Action #1b

Chief, Criminal Investigation CI
Director, Strategy CI:S

Monitoring Plan for Corrective Action #1b

CI uses software packages such as Doors and Microsoft Project to monitor the development of the new CIECS system. In addition, Business Systems Planning (BSP) assigned a Project Manager to oversee system development. CI conducts meetings with the contractor every two weeks to monitor their progress.

Management Advisory Report: Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service

Attachment

Management Response to "Management Advisory Report: Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service" (Audit No. 200110057)

Recommendation #2

Periodically generate from the inventory systems a report of all items of inventory that are recorded as status code "16" to ensure prompt and accurate action on these items, including a full investigation when warranted.

Assessment of Cause

The IRS is not consistent in the way we investigate missing computers.

Corrective Action #2

The Director, Enterprise Systems Asset Management, will generate a monthly report of all status code "16" inventory items, and will monitor to ensure prompt and accurate action on these items, including a full investigation when warranted.

Implementation Date of Corrective Action #2

Completed:

Proposed: January 1, 2002

Responsible Official for Corrective Action #2

Deputy Commissioner for Modernization and Chief Information Officer M
Chief Information Technology Services M:I
Director Enterprise Systems Asset Management M:I:M

Monitoring Plan for Corrective Action #2

Monthly, the Director, Enterprise Systems Asset Management, will assess the implementation and effectiveness of this process.

Management Advisory Report: Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service

Attachment

Management Response to "Management Advisory Report: Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service" (Audit No. 200110057)

Recommendation #3

Provide written guidance on the types of lost or stolen equipment that should be referred to TIGTA.

Assessment of Cause #3a

The IRS has written procedures requiring it to notify TIGTA regarding lost and stolen equipment (i.e., computers). Attachment 2 shows procedures published as a draft IRM and implemented in October 2001 as part of the improved disposal process.

Corrective Action #3a

Not Applicable.

Implementation Date of Corrective Action #3a

Not Applicable.

Responsible Official for Corrective Action #3a

Deputy Commissioner for Modernization and Chief Information Officer M
Chief Information Technology Services M:I
Director Enterprise Systems Asset Management M:I:M

Monitoring Plan for Corrective Action #3a

Not Applicable.

Management Advisory Report: Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service

Attachment

Management Response to "Management Advisory Report: Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service" (Audit No. 200110057)

Assessment of Cause #3b

Current guidelines require referral to TIGTA based on dollar criteria or a management finding of employee misconduct.

Corrective Action #3b

CI will revise the manual to provide guidance on the types of lost or stolen equipment that management should refer to TIGTA.

Implementation Date of Corrective Action #3b

Completed:

Proposed: December 1, 2002

Responsible Official for Corrective Action #3b

Chief, Criminal Investigation CI
Director, Operations and Policy Support CI:OPS

Monitoring Plan for Corrective Action #3b

CI will accomplish this through program reviews.

Management Advisory Report: Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service

Attachment

Management Response to "Management Advisory Report: Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service" (Audit No. 200110057)

Attachment 2

Revision of Section 1.5 IRM SPIF Procedure Excess And Disposal of IT Property

No matter where the equipment was or is located, if it has been determined that it has been lost, stolen, or damaged, IT will notify the appropriate security and investigative officials, if necessary, and prepare a Form 1933, Report of Survey, to Treasury Inspector General for Tax Administration (TIGTA) with a copy to Facilities Management. If there is no suspicion of criminal activity, IT will prepare the Form 1933 with an appropriate justification statement for the lost or damaged equipment. IT Management will approve and sign the Report of Survey prior to forwarding it to the local Facilities Management Official. The IRS Report No. format should be: RS-XXXX-XX-XXX (Note: Same format as referenced in Paragraph 2.g) above, except use RS for Report of Survey instead of EX, Excess. The ending number is incremented for each form prepared); e.g., RS-1101-01-001). After coordination with FMO for the disposition designation and determination that there is no criminal activity investigation, the SPIF will modify the equipment records with a Disposition Code of 00. FMO will perform the final disposal action with the appropriate Disposal Code.

Besides these draft procedures, we have also published procedures in IRM - Part II - Data Processing Services, Handbook 2.2.8 IS Operations Support Handbook, Subsection 1.11.2 Reporting **Lost** or Missing Magnetic Media to Inspection where it states:

- 1) The prompt reporting of missing or lost magnetic media is essential. Report missing and lost magnetic media to Inspection. Inspection, however, because of the volumes of media, does not want to receive routine information in every instance of lost or missing media. Call Inspection if management believes the loss was intentional or theft. Inspection believes that local management would best handle routine or inadvertent losses.

Note: Even if we did not have these draft IRM procedures, all computers contain magnetic media (hard drives), and in fact, it was the hard drives and classified information that might be contained on those hard drives, that was the subject of this review. Accordingly, the formerly published magnetic media reporting process covered the loss or theft of a computer (and its media).